537,671

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051458 A2

(51) International Patent Classification⁷: G06F 7/58

(21) International Application Number: PCT/IB2003/005265

(22) International Filing Date: 18 November 2003 (18.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/431,341 5 December 2002 (05.12.2002) US

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MITCHUM, Sam** [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). **EHRHARDT, Jack** [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). **LESTER, Bill** [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(74) Common Representative: **KONINKLIJKE PHILIPS ELECTRONICS N.V.**; c/o WAXLER, Aaron, P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

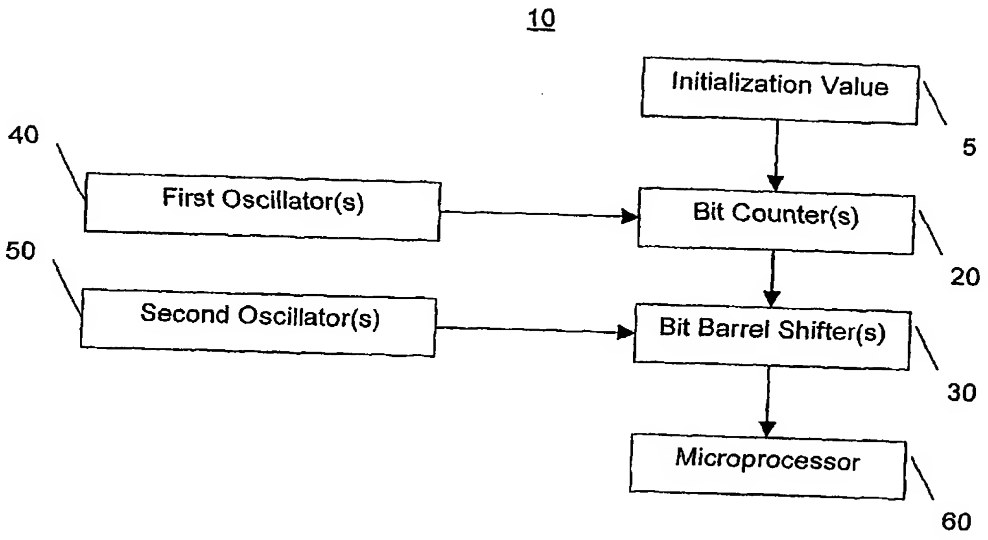
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR TRUE RANDOM NUMBER GENERATION



(57) Abstract: There is provided a system and method for providing an entirely digital and/or digitally synthesizable true random number generator for incorporation on integrated circuits using any standard logic synthesis tool or comparable technique. The system and method has at least a microprocessor operating at a first frequency, at least one counter for generating bits, at least one shifter for scrambling bits, at least one first oscillator for cooperating with the at least one counter; and at least one second oscillator for cooperating with the at least one shifter. The system being configured to provide a frequency perturbation based on digital input signals initialized via the microprocessor.

WO 2004/051458 A2

SYSTEM AND METHOD FOR TRUE RANDOM NUMBER GENERATION

The present invention relates to a method for providing a true random number generator. More particularly, the present invention relates to a system and method for providing an entirely digital and/or digitally synthesizable true random number generator for incorporation on integrated circuits (IC) using any standard logic synthesis tool or comparable technique.

Random number generation is employed in a variety of applications, including for example, computer security, cryptography, audio systems testing, bit error testing and secure communications. Current efforts in the area of random number generation typically require an analog oscillator to obtain frequency variance, or metastable flip flops to provide an unpredictable pattern, or analog circuitry to filter and amplify thermal noise, or some combination of each. Accordingly, it is desirable to provide a system and/or method for designing true random number generators (TRNGs) that do not require any of the aforementioned analog components and/or metastable configurations. It is also desirable for the system and/or method to facilitate the synthesis of TRNGs for incorporation on an IC using any standard technique.

It is an object of the present invention to provide a system and method for generating a true random number. The system and method comprise providing at least a counter, a shifter, a first oscillator for cooperating with the counter, a second oscillator for cooperating with the shifter, and a microprocessor for cooperating with each of the aforesaid components.

The system and method of the present invention provides for the generation of a random number without the use of analog clocks or metastable configurations because the generating clocks of the present invention are digitally controlled ring oscillators designed with frequency perturbation based on digital (high or low) input signals thereby allowing random frequencies to be generated from truly digital signals. Accordingly, random numbers can be generated using simple counters and shifters. TRNGs designed using the system and method of the present invention can be synthesized for incorporation on an IC using any standard logic synthesis tool or comparable technique. These and other objects and advantages of the present invention are achieved by the system and method of the present invention.

The present invention is more fully understood by reference to the following detailed description of an illustrative embodiment in combination with the drawings identified below.

Fig. 1 is a block diagram of a system in accordance with an illustrative embodiment of the present invention;

Fig. 2 is a block diagram of another illustrative embodiment of the present invention;

Fig. 3 is a schematic diagram of a true random number generating circuit in accordance with an illustrative embodiment of the present invention; and

Fig. 4 is a flow chart of one method for providing a true random number in accordance with the present invention.

Conventional systems for generating random numbers employ oscillators, such as ring oscillators to generate random numbers. Ring oscillators typically have an odd number of gates that are connected in series to form a ring, and in some cases a gate of such ring oscillators may have as an input a combination of outputs of other gates in the ring. Ring oscillators can be sampled at a certain point to provide a random or a pseudo random number.

Although conventional TRNGs can provide random numbers and/or pseudo random numbers, it is realized by those in the art that many of these TRNGs can be periodic in nature and consequently generate numbers that are less random than desirable. Further, as it is desirable to efficiently incorporate TRNGs on a chip or an IC so as to not require special components on the chip or IC to generate random numbers, a system that is relatively compact and that dissipates relatively small amounts of power is desirable.

The system and method of the present invention will be described hereafter in terms of certain illustrative embodiments. However, it will be recognizable to one of ordinary skill in the art that the system and method can effectively operate using other substitutable components and/or other comparable configurations.

Referring to the drawings and, in particular Fig. 1, there is shown a block diagram of a system for true random number generation in accordance with an illustrative embodiment of the present invention generally represented by reference numeral 10. Preferably, system 10 can accommodate at least a 2 Mbits/sec (62,500 numbers per second) rate while providing unpredictable/non-deterministic number generation, and can optionally operate with or without a seed value. System 10 is preferably biased against long runs of digital 0's and digital 1's. System 10 preferably can also have a sleep mode to reduce required power requirements.

System 10 has at least one counter 20 for generating bits, at least one shifter 30 for scrambling bits, at least one first oscillator 40 for cooperating with said at least one counter 20, at least one second oscillator 50 for cooperating with said at least one shifter 30, and a microprocessor 60 for cooperating with each of the aforesaid components to provide a frequency perturbation based on digital input signals. Counter 20 preferably has an initialization register for receiving an initialization bit value 5, the bit value preferably being inserted at a trailing edge of an initialization write of microprocessor 60. Counter 20 is preferably a 32-bit up counter. However, counter 20 can also be 16-bit up counter and a 16-bit down counter, and/or any other comparable type of counter suitable for accomplishing the above-identified objects of the present invention. If the 16-bit counters are used, the outputs thereof may be interleaved into shifter 30. Shifter 30 preferably being a barrel shifter, and more particularly a 32-bit barrel shifter. Shifter 30 can be any other comparable type of shifter suitable for accomplishing the above-identified objects of the present invention. First and second oscillators 40 and 50 are preferably ring oscillators each having a differing odd number of stages, first oscillator 40 preferably being a 5-stage oscillator and second oscillator 50 preferably being a 7-stage oscillator. It is noted however, that first and second oscillators 40 and 50, respectively, can also be any other comparable type of oscillator sufficient to accomplish the above-identified objects of the present invention. First and second oscillators 40 and 50 can preferably be constructed from a combination of inverters, AND gates, NAND gates, NOR gates, XOR gates, and/or any other similar type components. Refer generally to Fig. 3 for one illustrative embodiment of system 10 employing an illustrative combination of components in accordance with the present invention.

Referring to Fig. 2, system 10 can preferably include a whitening filter and/or a linear feedback shift register ("LFSR") 70 between shifter 30 and microprocessor 60. This arrangement preferably facilitates using a counter value to modify an output of shifter 30. Preferably, LFSR 70 can have any number of stages appropriate for accomplishing the above-identified objectives of the present invention. System 10 can also include a one-hot shift selector 80 between second oscillator 50 and shifter 30.

To illustrate how system 10 operates, refer to Fig. 4, which is a flow chart of one method for providing a true random number in accordance with an illustrative embodiment of the present invention generally represented by reference numeral 100. Method 100 comprising at least the steps of 110, 120, 130 and 140. Step 110 is to utilize at least one counters 20 to generate bits. Preferably, counter 20 is initialized by a write from microprocessor 60 to an initialization register of the counter, the microprocessor having some rate or frequency. Preferably, counter 20 is clocked by first oscillator 40 at a rate or frequency that is preferably chip dependent on the physical characteristics of the components used to form the first oscillator and asynchronous to that of the microprocessor. Step 120 is to utilize at least one shifter 30 to scramble bits. Preferably, shifter 30 cooperates with counter 20, shifter 30 being continuously spun by second oscillator 50 at a rate or frequency asynchronous to that of counter 20 and microprocessor 60. Preferably, the shifter rate or frequency is faster than that of the microprocessor. Step 130 is to utilize oscillators 40 and 50 to simultaneously cooperate with counter 20 and shifter 30, respectively. Step 140 is to cross couple asynchronous frequency control bits for oscillators 40 and 50 from counter 20 and shifter 30. Accordingly, it is preferable that when microprocessor 60 reads a random number having a certain number of bits, such as for example 32 bits, shifter 30 will preferably inputs a current counter 20 value and shift it by a current shift count (e.g. 0 to 31). Preferably, as the frequencies of each of components (i.e., the counter, the shifter and the microprocessor) are asynchronous to each other, a non-predictable pattern of bit numbers is returned to the microprocessor.

The present invention having been thus described with particular reference to the preferred forms thereof, it will be obvious that various changes and modifications may be made therein without departing from the spirit and scope of the present invention as defined herein.

CLAIMS:

1. A system for generating a true random number comprising:

a microprocessor operating at a first frequency,

at least one counter for generating bits;

at least one shifter for scrambling bits;

at least one first oscillator for cooperating with said at least one counter; and

at least one second oscillator for cooperating with said at least one shifter,

wherein said oscillators provide a frequency perturbation based on digital input signals initialized via said microprocessor.

2. The system of claim 1, wherein said counter has an initialization register for receiving an initialization bit value.

3. The system of claim 2, wherein said initialization bit value is at a trailing edge of an initialization write of said microprocessor.

4. The system of claim 3, wherein said at least one first oscillator is a ring oscillator having a first odd number of stages.

5. The system of claim 4, wherein said at least one first ring oscillator is cooperates with said at least one counter to provide a second frequency.

6. The system of claim 5, wherein said at least one shifter is a barrel shifter being continuously spun by said at least one second oscillator at a third frequency.

7. The system of claim 6, wherein said at least one second oscillator is a ring oscillator having a second odd number of stages differing from said first odd number of stages by at least two stages.

8. The system of claim 7, wherein said third frequency is asynchronous to said second frequency.

9. The system of claim 8, wherein said third frequency is asynchronous to said first frequency.

10. The system of claim 8, wherein said third frequency is asynchronous to and faster than said first frequency.

11. The system of claim 9, wherein said counter is timed or clocked at said second frequency with said second frequency being asynchronous to said third frequency.

12. The system of claim 11, wherein said second frequency is asynchronous to said first frequency.

13. The system of claim 12, wherein when said microprocessor reads a random number, said barrel shifter inputs a current counter bit value and shifts said bit value by a current barrel shift count.

14. A method for providing a true random number generator comprising the steps of:

(a) providing a microprocessor operating at a first frequency;

(b) providing at least one counter;

(c) providing at least one first oscillator to clock said at least one counter at a second frequency;

(d) providing at least one shifter; and

(e) providing at least one second oscillator for continuously spinning said at least one shifter at a third frequency.

15. The method of claim 13, wherein said at least one first oscillator has a first odd number of stages and said second oscillator has a second odd number of stages differing from said first odd number of stages by at least two stages.

16. The method of claim 13, wherein said first frequency, said second frequency and said third frequency are each asynchronous to each other.

17. The method of claim 15, wherein when said microprocessor reads a random number, said shifter inputs a current counter bit value and shifts said bit value by a current shift count.

18. A method for generating a true random number comprising the steps of:

(a) providing a microprocessor operating at a first frequency, at least one counter for generating bits, at least one shifter for scrambling bits, a first and second oscillator for cooperating with said counter and said shifter, respectively;

(b) initializing said counter by a write of said microprocessor to an initialization register of said at least one counter;

(c) clocking said at least one counter via said first oscillator at a second frequency;

(d) continuously spinning said at least one shifter via said second oscillator at a third frequency;

(e) inputting a current counter bit value, at a time when said microprocessor reads a random bit number, and shifting said current bit value by a current shift count; and

(f) returning said shifted bit value to said microprocessor to achieve a non-predictable pattern of bit numbers.

19. The method of claim 17, wherein said at least one first oscillator has a first odd number of stages and said second oscillator has a second odd number of stages differing from said first odd number of stages by at least two stages.

20. The method of claim 17, wherein said first frequency, said second frequency and said third frequency are each asynchronous to each other.

21. The method of claim 19, wherein when said microprocessor reads a random number, said shifter inputs a current counter bit value and shifts said bit value by a current shift count.

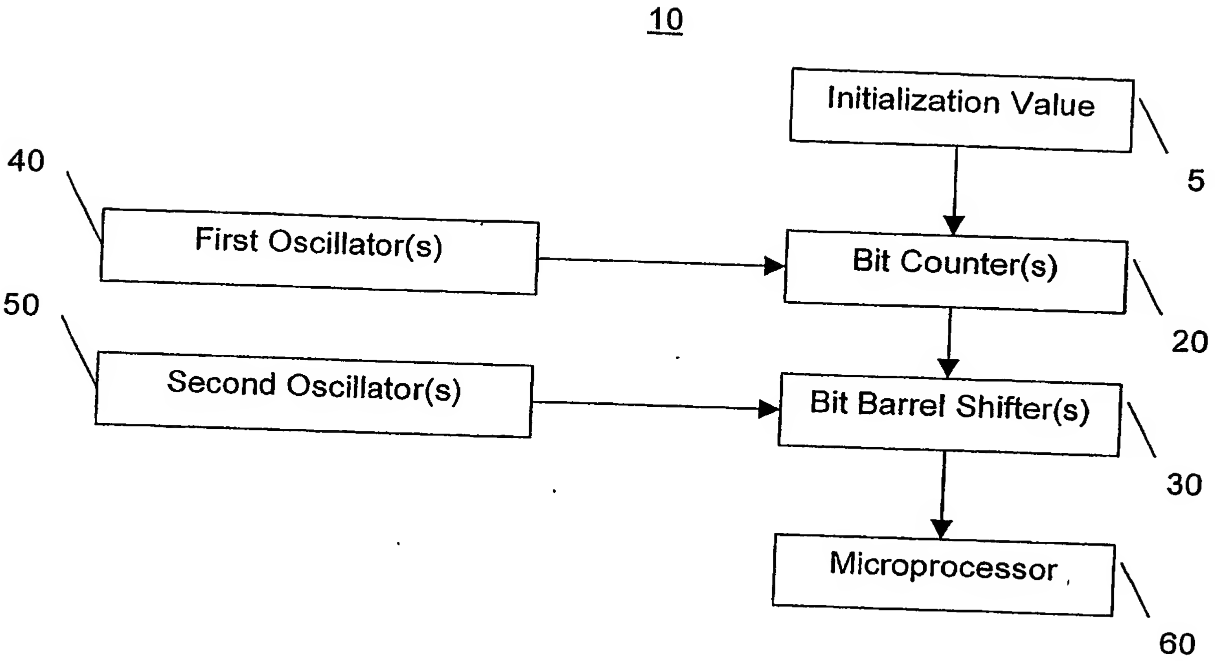

10
Initialization Value
5
40
First Oscillator(s)
Bit Counter(s)
20
50
Second Oscillator(s)
Bit Barrel Shifter(s)
30
Microprocessor
60

FIG. 1

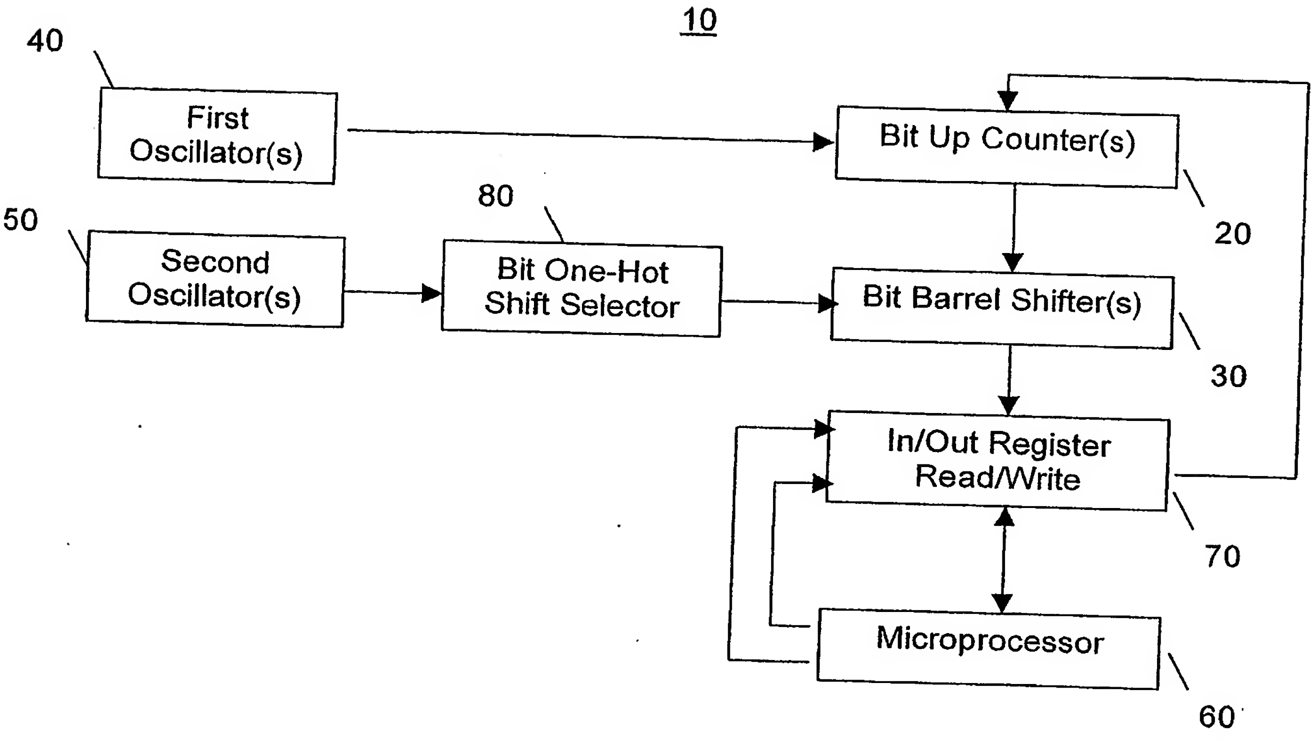

10
40
First Oscillator(s)
50
Second Oscillator(s)
80
Bit One-Hot Shift Selector
Bit Up Counter(s)
20
Bit Barrel Shifter(s)
30
In/Out Register Read/Write
70
Microprocessor
60

FIG. 2

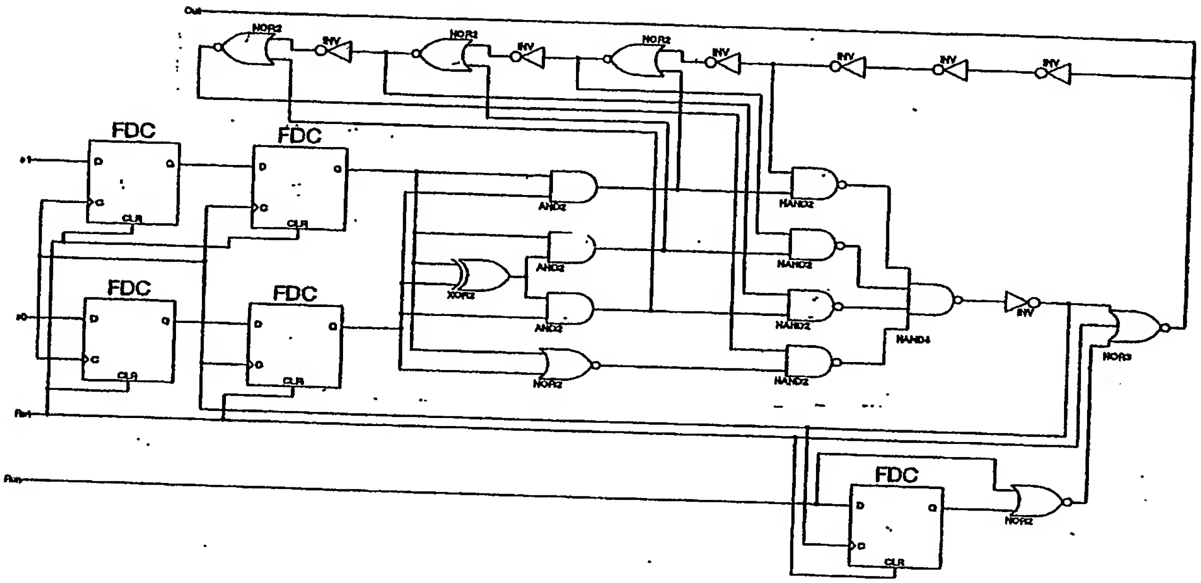

Out
NOR2
INV
NOR2
INV
NOR2
INV
INV
INV
INV
FDC
FDC
s1
D
Q
C
CLR
AND2
NAND2
AND2
XOR2
NAND2
FDC
FDC
s0
AND2
NAND2
NAND4
INV
NOR3
NOR2
NAND2
Rst
FDC
Run
NOR2

FIG. 3

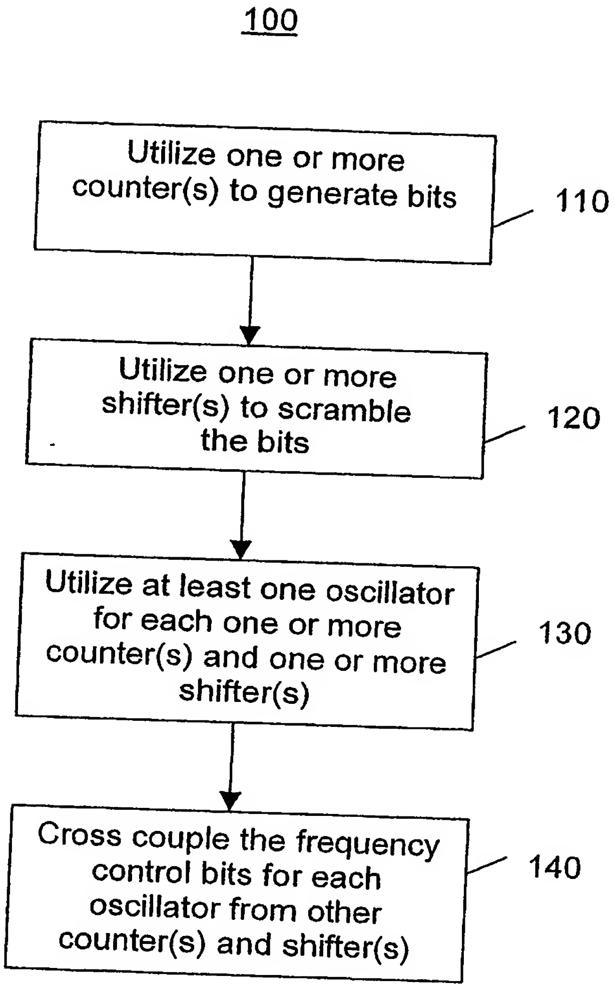

100
Utilize one or more counter(s) to generate bits
110
Utilize one or more shifter(s) to scramble the bits
120
Utilize at least one oscillator for each one or more counter(s) and one or more shifter(s)
130
Cross couple the frequency control bits for each oscillator from other counter(s) and shifter(s)
140

FIG. 4

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property
Organization
International Bureau

(43) International Publication Date
17 June 2004 (17.06.2004)

PCT

(10) International Publication Number
WO 2004/051458 A3

(51) International Patent Classification⁷: G06F 7/58

(21) International Application Number: PCT/IB2003/005265

(22) International Filing Date: 18 November 2003 (18.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/431,341 5 December 2002 (05.12.2002) US

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **MITCHUM, Sam** [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). **EHRHARDT, Jack** [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US). **LESTER, Bill** [US/US]; P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

(74) Common Representative: **KONINKLIJKE PHILIPS ELECTRONICS N.V.**; c/o WAXLER, Aaron, P.O. Box 3001, Briarcliff Manor, NY 10510-8001 (US).

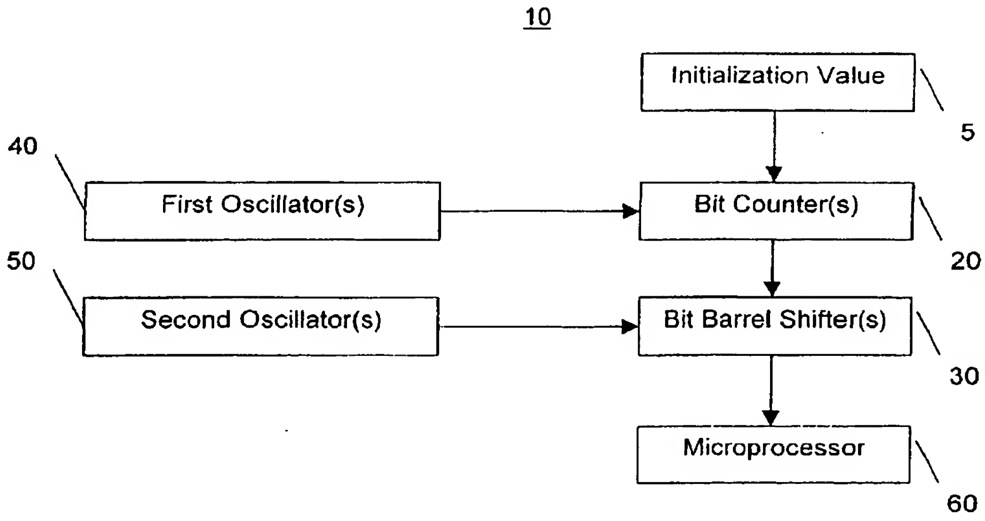
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:
— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for all designations*

[Continued on next page]

(54) **Title:** SYSTEM AND METHOD FOR TRUE RANDOM NUMBER GENERATION



(57) **Abstract:** There is provided a system and method for providing an entirely digital and/or digitally synthesizable true random number generator for incorporation on integrated circuits using any standard logic synthesis tool or comparable technique. The system and method has at least a microprocessor operating at a first frequency, at least one counter for generating bits, at least one shifter for scrambling bits, at least one first oscillator for cooperating with the at least one counter; and at least one second oscillator for cooperating with the at least one shifter. The system being configured to provide a frequency perturbation based on digital input signals initialized via the microprocessor.

Published:

- *with international search report*
- *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
2 December 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.